CLAIMS

1. A semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit, in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents;

wherein said second storage means has an externally readable area that can be read from the outside of the semiconductor integrated circuit, and an externally unreadable area that cannot be read from the outside; and

after arbitrary data is stored in the externally readable area of the second storage means, the data is read to the outside of the semiconductor integrated circuit to check whether the arbitrary data is the data as inputted, and thereafter, the rewrite program read from the first storage means is stored in the externally unreadable area of the second storage means.

2. A semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit, in which a program that makes an arithmetic processing unit in the

semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents, said semiconductor integrated circuit device including:

a control circuit for performing control so as to read only a specific portion of the rewrite program stored in the second storage means.

3. A semiconductor integrated circuit device as defined in Claim 2 wherein said control circuit performs control so as to read only the rewrite program located in specific addresses of the second storage means.

4. A semiconductor integrated circuit device as defined in Claim 2 wherein said control circuit performs control so as to read only specific bits of the rewrite program stored in the second storage means.

5. A semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit, in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of

processing contents is rewritably stored, and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents;

wherein said rewrite program includes a program for executing a portion of the rewrite program after the rewriting; and

the portion of the rewrite program stored in the second storage means is executed.

6. A semiconductor integrated circuit device as defined in Claim 5 wherein the portion of the rewrite program to be executed is one for successively executing discontinuous program areas.

7. A semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit, in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents; and

said semiconductor integrated circuit device including, in the semiconductor integrated circuit, a transfer monitor means

for monitoring the rewrite program to be transferred from the first storage means to the second storage means.

8. A semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit, in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting of the program stored in the second storage means using a first storage means in which a rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents;

wherein the rewrite program includes a check program for checking whether the program is correct or not;

the semiconductor integrated circuit is provided with a work memory for the arithmetic processing unit, and a connection switching means for switching the connection between the second storage means or the work memory, and the program input or the data input of the arithmetic processing unit; and

the check program that is extracted from the rewrite program stored in the second storage means is stored in the work memory, and the arithmetic processing unit is operated by the check program stored in the work memory, thereby to check whether the rewrite program is correct or not.

9. A semiconductor integrated circuit device as defined in Claim 8 wherein the second storage means holds the rewrite program, and holds data which is uniquely obtained from a predetermined cluster in the rewrite program, according to a predetermined rule.

10. A semiconductor integrated circuit device as defined in Claim 9 wherein the uniquely obtained data is used as a check code for checking whether the program is correct or not.

11. A semiconductor integrated circuit device as defined in Claim 8 wherein

the second storage means has a construction in which an area where the rewrite program is not stored is successively divided into two areas, and the same program is stored in each of the two areas;

the check program includes

a program for comparing the program data stored in one of the two areas with the same data stored in the other area, thereby to check whether the program data is correct or not, and

a program for, when the result of the previous check is that the program data is correct, repeating an operation of further dividing one of the two areas, as an area wherein no program is stored, into two areas, and storing the same program data in each of the two areas; and

all of the programs to be stored in the second storage means

are successively stored.

12. A semiconductor integrated circuit device as defined in Claim 11 wherein the second storage means stores the rewrite program data, and data that is uniquely obtained from the program data according to a predetermined rule, in the two areas into which the area in the second storage means where the rewrite program is not stored is successively divided.

13. A semiconductor integrated circuit device as defined in Claim 12 wherein the uniquely obtained data is inverted data of the program data.

14. A semiconductor integrated circuit device as defined in any of Claims 8 to 13 further including a ROM (Read Only Memory) in which the check program is previously stored;

wherein the arithmetic processing unit is operated by the ROM to check whether the rewrite program is correct or not.

15. A semiconductor integrated circuit device as defined in any of Claims 1 to 14 further including, in the semiconductor integrated circuit, a decryption means for decrypting the encrypted rewrite program;

wherein, when the rewrite program stored in the first storage means has previously been encrypted, the decryption means

decrypts the encrypted program, and stores the decrypted rewrite program in the second storage means.

16. A semiconductor integrated circuit device having a second storage means in a semiconductor integrated circuit, in which a program that makes an arithmetic processing unit in the semiconductor integrated circuit perform an operation of processing contents is rewritably stored, and performing rewriting using a first storage means in which a previously encrypted rewrite program for rewriting is stored, which rewrite program makes the arithmetic processing unit perform an operation of processing the contents;

said semiconductor integrated circuit device including, in the semiconductor integrated circuit,

a decryption means for decrypting the encrypted rewrite program read from the first storage means, and transferring the decrypted rewrite program to the second storage means; and

an encryption means for again encrypting the rewrite program stored in the second storage means;

wherein the rewrite program encrypted by the encryption means is compared with the encrypted rewrite program stored in the first storage means.

17. A semiconductor integrated circuit device as defined in any of Claims 11 to 13 and 16 wherein, when data are not correctly

stored in the second storage means, a defective portion is detected, and the rewrite program stored in the first storage means is corrected.

18. A semiconductor integrated circuit device as defined in any of Claims 1 to 17 wherein the rewrite program that is stored outside the semiconductor integrated circuit device is downloadable into the semiconductor integrated circuit.

19. A data storage verification device comprising:

means for storing arbitrary data in an area which is accessible from the outside;

means for outputting the arbitrary data to the outside, and judging whether the arbitrary data is correctly stored or not; and

means for storing secret data in an area which is inaccessible from the outside, when it is judged that the arbitrary data is correctly stored.

20. A data storage verification device comprising:

means for storing secret data in an area which is inaccessible from the outside; and

means for outputting a specific portion of the secret data to the outside.

21. A data storage verification device comprising:

means for storing secret data including a program in an area which is inaccessible from the outside; and

means for executing the stored program, and outputting the result to the outside.

22. A data storage verification device comprising:

first means for storing secret data including an inspection program and a secret program into an area which is inaccessible from the outside;

second means for executing the inspection program, and outputting the result to the outside; and

third means for executing the secret program after completion of the second means.

23. A data storage verification device comprising:

means for storing secret data in an area which is inaccessible from the outside;

means for performing a predetermined arithmetic operation using the secret data, simultaneously with the storage; and

means for outputting the result of the arithmetic operation to the outside.

24. A data storage verification device comprising:

fourth means for storing secret data in a first area which is

inaccessible from the outside;

fifth means for storing an inspection program which is a part of the secret data and is stored in the first area, into a second area; and

sixth means for executing the inspection program stored in the second area to verify correctness of the secret data stored in the first area.

25. A data storage verification device as defined in Claim 24 further including seventh means for transferring control to a command of the first area after completion of the sixth means.

26. A data storage verification device as defined in Claim 24 wherein the fifth means executes storage of the inspection program according to a command that exists in the secret data stored in the first area.

27. A data storage verification device as defined in Claim 24 wherein the fifth means executes the inspection program according to a command that has been stored in a third area before execution of storage by the fourth means.

28. A data storage verification device comprising:

means for decrypting secret data;

means for storing the decrypted data in an area which is

inaccessible from the outside;

means for encrypting the stored data; and

means for comparing the encrypted data with the secret data to judge whether the stored data is correctly stored or not.

29. A data storage verification device comprising:

21st means for storing secret program in an area which is inaccessible from the outside;

22nd means for reading the stored program;

23rd means for judging correctness of the read program for each command unit;

24th means for again storing a correct command in an empty area in the area that is inaccessible from the outside, when it is judged that the read program is incorrect;

25th means for storing a command for making a command next to the again-stored command jump to an address next to the address that is judged as incorrect; and

26th means for storing, in the area that is judged as incorrect, a command for making a jump to the address of the again-stored command.

30. A data storage verification method comprising:

step of storing arbitrary data in an area which is accessible from the outside;

step of outputting the arbitrary data to the outside, and

judging whether the arbitrary data is correctly stored or not; and

step of storing secret data in an area which is inaccessible from the outside, when it is judged that the arbitrary data is correctly stored.

31. A data storage verification method comprising:

step of storing secret data in an area which is inaccessible from the outside; and

step of outputting a specific portion of the secret data to the outside.

32. A data storage verification method comprising:

step of storing secret data including a program in an area which is inaccessible from the outside; and

step of executing the stored program, and outputting the result to the outside.

33. A data storage verification method comprising:

first step of storing secret data including an inspection program and a secret program into an area which is inaccessible from the outside;

second step of executing the inspection program, and outputting the result to the outside; and

third step of executing the secret program after completion

of the second step.

34. A data storage verification method comprising:

step of storing secret data in an area which is inaccessible from the outside;

step of performing a predetermined arithmetic operation using the secret data, simultaneously with the storage; and

step of outputting the result of the arithmetic operation to the outside.

35. A data storage verification method comprising:

fourth step of storing secret data in a first area which is inaccessible from the outside;

fifth step of storing an inspection program which is a part of the secret data and is stored in the first area, into a second area; and

sixth step of executing the inspection program stored in the second area to verify correctness of the secret data stored in the first area.

36. A data storage verification method as defined in Claim 36 further including seventh step of transferring control to a command of the first area after completion of the sixth step.

37. A data storage verification method as defined in Claim 35

wherein the fifth step executes storage of the inspection program according to a command that exists in the secret data stored in the first area.

38. A data storage verification method as defined in Claim 35 wherein the fifth step executes the inspection program according to a command that has been stored in a third area before execution of storage in the fourth step.

39. A data storage verification method comprising:

step of decrypting secret data;

step of storing the decrypted data in an area which is inaccessible from the outside;

step of encrypting the stored data; and

step of comparing the encrypted data with the secret data to judge whether the stored data is correctly stored or not.

40. A data storage verification method comprising:

step of storing secret program in an area which is inaccessible from the outside;

step of reading the stored program;

step of judging correctness of the read program for each command unit;

step of again storing a correct command in an empty area in the area that is inaccessible from the outside, when it is judged

that the read program is incorrect;

step of storing a command for making a command next to the again-stored command jump to an address next to the address that is judged as incorrect; and

step of storing, in the area that is judged as incorrect, a command for making a jump to the address of the again-stored command.